

REMARKS

Summary of Office Action

Claims 1-5 and 7-16 were pending.

Claim 17 was previously withdrawn from consideration as drawn toward a non-elected invention.

Claim 1 has been rejected under 35 U.S.C. § 112, second paragraph. Further, claims 1-5 and 7-16 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Breck et al. U.S. patent application Publication No. 2004/0210449).

Applicants' Reply

Applicants respectfully traverse the § 112 rejection. Applicants note the allegedly indefinite term: "that code", clearly refers to the precedent term: "the second acquirer code", which is recited in the same phrase. However, for further clarity, applicants have amended claim 1 to explicitly replace "that" code with "the included second acquirer" code. Claim 1 now conforms to all requirements of § 112.

Applicants respectfully traverse the prior art rejections.

Applicants note that cited reference —Breck, is unrelated to subject matter of applicants' claims. Breck relates to the use of a "dummy" or "proxy" number (i.e., Secure transaction number (STN) 15) in lieu of a cardholder's actual or primary account number (PAN) for payment transaction processing, which involves a card holder, a merchant and an issuer (card provider). (See FIGS. 1 and 8, ¶¶ [0048], [0052], [0053], [0054], [0058], [0059], [0066], [0074], [0076]-[0083], and [0090]). The payment processing between the merchant and the issuer/card provider (i.e., step 115, FIGS. 1 and 8) is conventional except for the replacement of the PAN by the dummy STN 15. (See e.g., ¶ [0054], and ¶ [0081]): "the merchant 2 submits an authorization request to the card provider 3, as it would with any other credit card transaction").

Breck does not relate to, and fails to show applicants' inventive modifications and improvements over conventional payment processing (e.g., authorization request processing) between merchant and issuer.

Claim 1

The elements of claim 1 include:

(a) receiving by a service provider other than an issuer of the payment account a first authorization request for the authorization of the transaction using a first payment account number, wherein:

(i) the first payment account number has a service provider identification number that is associated with the service provider other than the issuer and is associated with a second payment account number that has an issuer identification number associated with the issuer, said second payment account number not being included in said first authorization request;

(ii) ...

(iii) the first authorization request is routable through the payment network to the service provider based on said service provider identification number;

(b) responsive to the first authorization request, transmitting by the service provider a second authorization request for authorization of the transaction using the second payment account number, the second authorization request including a second acquirer code associated with the service provider and being routable through the payment network to the issuer based on said issuer identification number;

(c) receiving from the issuer a response to the second authorization request transmitted by the service provider, the response including the second acquirer code and being routable through the payment network based on that code; and

(d) transmitting from the service provider to the acquirer a response to the first authorization request received by the service provider based on the response to the second authorization request received by the service provider from the issuer, the response to the first authorization request including the first acquirer code and being routable through the payment network based on that code.

Contrary to the assertion in the Office Action (page 3-4, section 7), Breck does not teach about the use of two different payment account numbers or a service provider's involvement in a hyphenated transaction processing between merchant, service provider and the issuer in the manner of applicants' claim 1.

In particular, Breck does not show “a first payment account number [that] has a service provider identification number that is associated with the service provider [and] a second payment account number that has an issuer identification number associated with the issuer, said second payment account number not being included in said first authorization request.”

Further, Breck does not mention or suggest a service provider, an acquiring bank or any other intermediate entity, which sends a second authorization request that according to claim 1 has a “second identification number associated with the issuer” and “a second payment account number [that is] not [] included in the first authorization request.”

For at least the foregoing reasons, claim 1 and its dependent claims 2-4 are patentable over Breck.

Claim 5

The elements of claim 5 include:

- (a) generating a message authentication code based on one or more transaction details;
- (b) transmitting at least the first payment account number and the message authentication code to the merchant;
- (c) requesting by the merchant an a first authorization request for payment of the transaction using the first payment account number, said second payment account number not being included in said first authorization request, the request being formatted as if payment were tendered at a point-of-sale terminal with a conventional magnetic-stripe payment card, the format having a track with at least a discretionary data field and said message authentication code being transmitted in said discretionary data field;
- (d) responsive to the authorization request for the first payment account number, requesting an authorization for payment of the transaction using the second payment account number; and
- (e) accepting or declining the authorization request for the first payment account number based on the response to the authorization request for the second payment account number and the message authentication code, wherein said first and second payment account numbers include respective service provider and issuer identification numbers, wherein a service provider other than the issuer receives said

merchant's request through a payment network based on said service provider identification number, and wherein said service provider generates said request for authorization of payment using the second payment account number and routes said request to said issuer through said network based on said issuer identification number.

Like claim 1, claim 5 requires a first authorization request from the merchant and a second authorization request from the service provider, the second authorization request transmitted by the service provider including a "second identification number" associated with "the issuer" and "a second payment account number that is not included in the first authorization request". As discussed above with respect to claim 1, these limitations are not shown by Breck.

Claim 5 also requires "a message authentication code being transmitted in said discretionary data field" of a magnetic stripe data structure format. Applicants note that Breck does not show this limitation. Breck does not deal with "message authentication codes," and in particular does not describe "a message authentication code being transmitted in said discretionary data field" which is required by claim 5.

For at least the foregoing reasons, claim 5 and its dependent claims 7-8 are not anticipated by and are patentable over Breck.

Claims 9 and 14

Claim 9 and claims 14 describe additional features of applicants' methods for secure payment transactions. In particular, these claims require computer generation of a message or transaction authentication code, which is positioned in the discretionary data field of a standard payment card track image and then transmitted over the electronic payment network.

Applicants submit that Breck does not show this feature of claims 9 and 14. Breck does not describe any standard payment card track image. As noted above in reference to claim 5, Breck does not deal with "message authentication codes." In particular, Breck does not describe positioning and transmitting a computer generated transaction/message authentication code in the discretionary data field of a standard payment card track image.

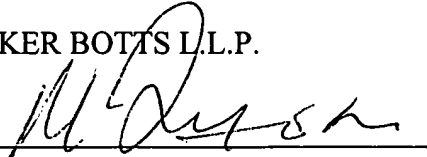
For at least this reason, claims 9 and 14 and their dependent claims 10-13 and 15-16, respectively, are patentable over the cited references.

Conclusion

In view of the foregoing remarks, favorable consideration and allowance of claims 1-16 are respectfully solicited. In the event that the application is not deemed in condition for allowance, the Examiner is requested to contact the undersigned in an effort to advance the prosecution of this application.

Respectfully submitted,

BAKER BOTTS L.L.P.



Dated: February 20, 2007

Manu J Tejawani
Patent Office Reg. No. 37,952

BAKER BOTTS L.L.P.
30 Rockefeller Plaza
New York, NY 10112-4498
Attorney for Applicants
212-408-2500

BAKER BOTTS LLP

Attorney Docket Number: 070457.1000 - AP33154

Title: METHOD AND SYSTEM FOR CONDUCTING SECURE PAYMENTS OVER A COMPUTER NETWORK



Use Space Below for Additional Information: